



# Securing IoT Devices with Manufacturer Usage Descriptions

Eliot Lear

Principal Engineer, Enterprise Chief Technology Office

10 Apr 2019

Today's latest  
threat: printers

**Study cites multi-function printers as  
some of the most dangerous members of  
the IoT family**



Bitdefender.com, 28 February 2019

# What Sort of Access Do These Printers Require?

From	To	Protocol	Source Port	Destination Port(s)
Printer	xmpp009.hpeprint.com	TCP		80, 443, 5222, 5223
Printer	DNS Server	UDP		53
Printer	chat.hpeprint.com	TCP		80, 443
Printer	224.0.0.251/32	UDP		5353
Printer	220.0.0.252/32	UDP		5355
Printer	h10141.www1.hp.com	TCP		80
Printer	Local Networks	UDP	5353	
Printer	Local Networks	TCP	80	

Source: University of New South Wales, using mudgee

(not shown: L2 packets)

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Our First Three Questions

- Is that information correct?
  - Maybe: Not sourced from vendor
- How does the administrator learn it?
  - Scanned network for some number of days
- What vulnerabilities does that device have?
  - Can't tell because we probably don't have model information

And consider how much time it will take for that one device.



# Assumptions and Assertions

## Assumptions

A Thing has a single use or a small number of uses.

Things are tightly constrained. Very little CPU, memory, and battery.

Network administrators are the ultimate arbiters of how their networks will be used

Even those Things that can protect themselves today may not be able to do so tomorrow

## Assertions

Because a Thing has a single or a small number of intended uses, all other uses must be unintended.

Any intended use can be clearly identified.

Manufacturers are in a generally good position to provide guidance to administrators.

A mechanism is needed to protect devices that may have vulnerabilities.

# Translating intent into config

Any intended use can be clearly identified by the manufacturer



```
access-list 10 permit host  
controller.mfg.example.com
```

All other uses can be warned against in a statement by the manufacturer



```
access-list 10 deny any any
```

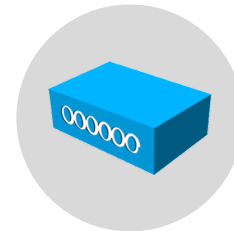


# Introducing Manufacturer Usage Descriptions (MUD)

A URL:

<https://manufacturer.example.com/mydevice.json>

The MUD Manager:



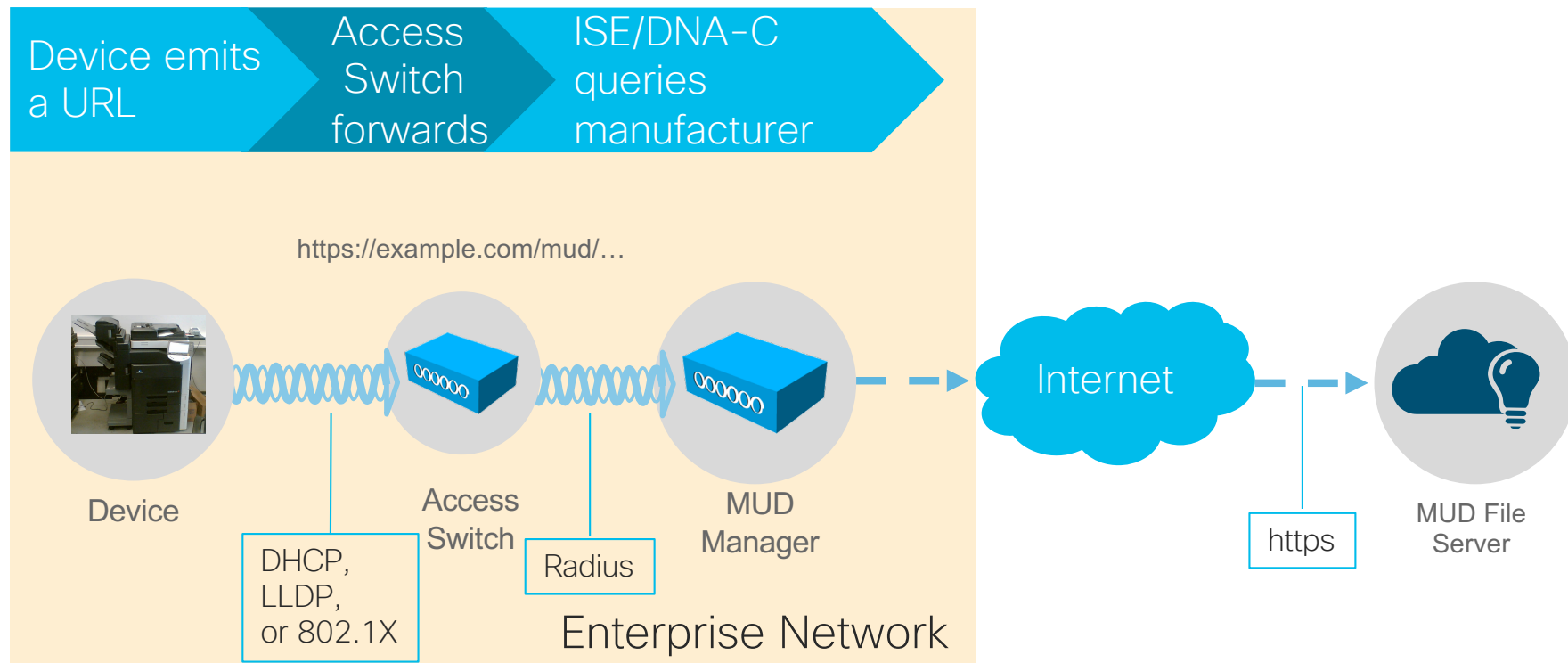
A MUD File:

```
...  
"ace": [ {  
  "name": "cl0-todev",  
  "matches": {  
    "ietf-mud:mud": {  
      "my-controller": [  
        null  
      ]  
    },  
  },  
  "actions": {  
    "forwarding": "accept"  
  } } ]  
...
```

The MUD File Server:

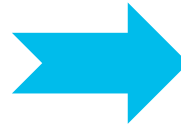


# Expressing Manufacturer Usage Descriptions



# Getting from the MUD file to deployment config

```
... "acl": [  
  {  
    "name": "mud-76228-v4to",  
    "type": "ipv4-acl-type",  
    "aces": {  
      "ace": [  
        {  
          "name": "myctl0-todev",  
          "matches": {  
            "ietf-mud:mud": {  
              "my-controller": [  
                null  
              ]  
            }  
          },  
          "actions": {  
            "forwarding": "accept"  
          }  
        }  
      ],  
      "actions": {  
        "forwarding": "accept"  
      }  
    }  
  ],  
  "actions": {  
    "forwarding": "accept"  
  }  
} ...
```



Whatever is appropriate  
in the local deployment.

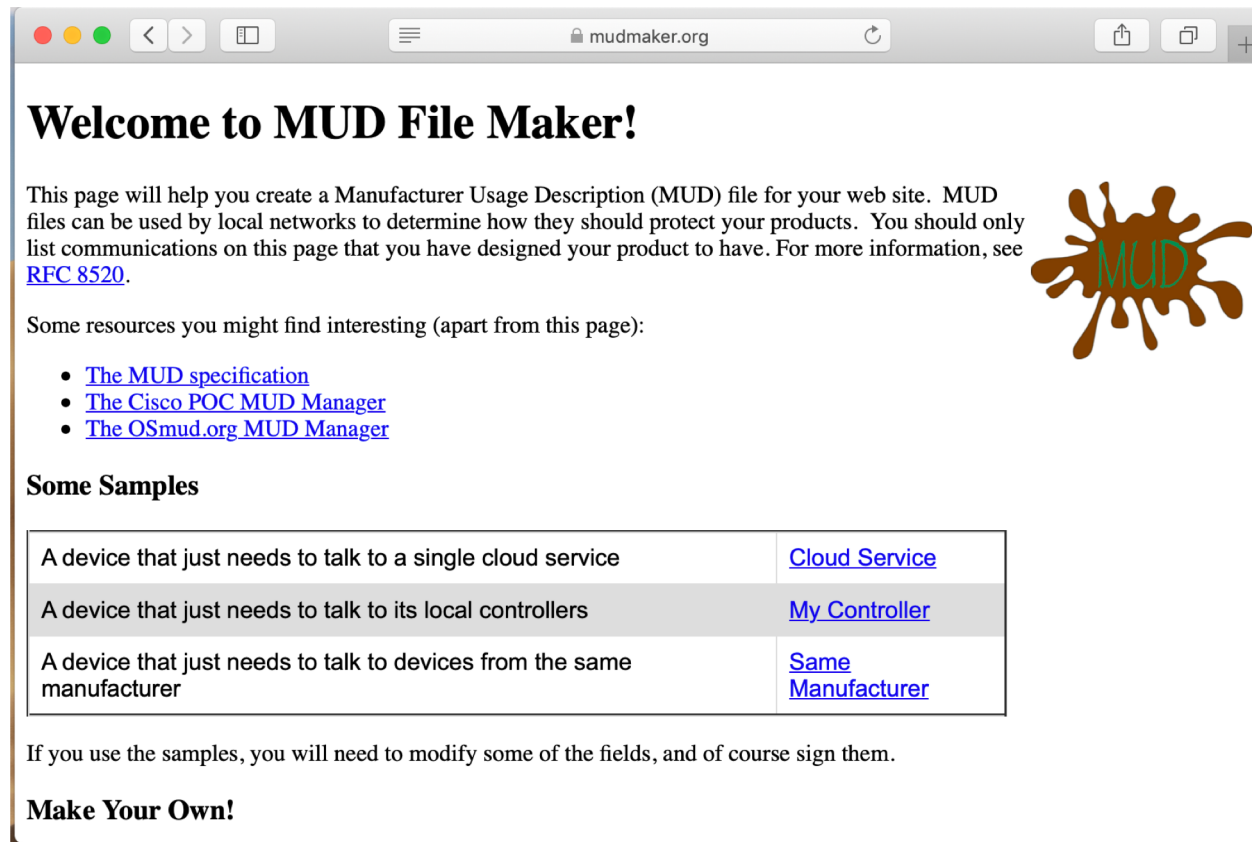
10.1.2.3  
10.4.5.6

<https://mudmaker.org>

# Manufacturers Use Classes

Class	Used for	Filled in by
Domain name	Cloud-based controllers	IOS
(My) Controller	Access to controllers	Administrator
same-manufacturer	Access to devices that are built by the same manufacturer	MUD Manager
Manufacturer	Access to devices that are built by specified manufacturer	Manufacturer and MUD Manager
Local	Used when device needs access to the local network	Administrator

# Make Your Own MUD File

A screenshot of a web browser window showing the mudmaker.org website. The browser's address bar displays 'mudmaker.org'. The page has a white background with black text. At the top, there's a heading 'Welcome to MUD File Maker!'. Below it, a paragraph explains the purpose of MUD files and includes a link to 'RFC 8520'. To the right of this text is a brown, splatter-like logo with the word 'MUD' in green. Further down, a section titled 'Some resources you might find interesting (apart from this page):' lists three links: 'The MUD specification', 'The Cisco POC MUD Manager', and 'The OSmud.org MUD Manager'. Below this is a section titled 'Some Samples' which contains a table with three rows. Each row describes a device configuration and provides a corresponding link. The table has a light gray background. At the bottom of the page, there's a paragraph stating that users will need to modify fields and sign them if they use the samples, followed by the heading 'Make Your Own!'.

**Welcome to MUD File Maker!**

This page will help you create a Manufacturer Usage Description (MUD) file for your web site. MUD files can be used by local networks to determine how they should protect your products. You should only list communications on this page that you have designed your product to have. For more information, see [RFC 8520](#).

Some resources you might find interesting (apart from this page):

- [The MUD specification](#)
- [The Cisco POC MUD Manager](#)
- [The OSmud.org MUD Manager](#)

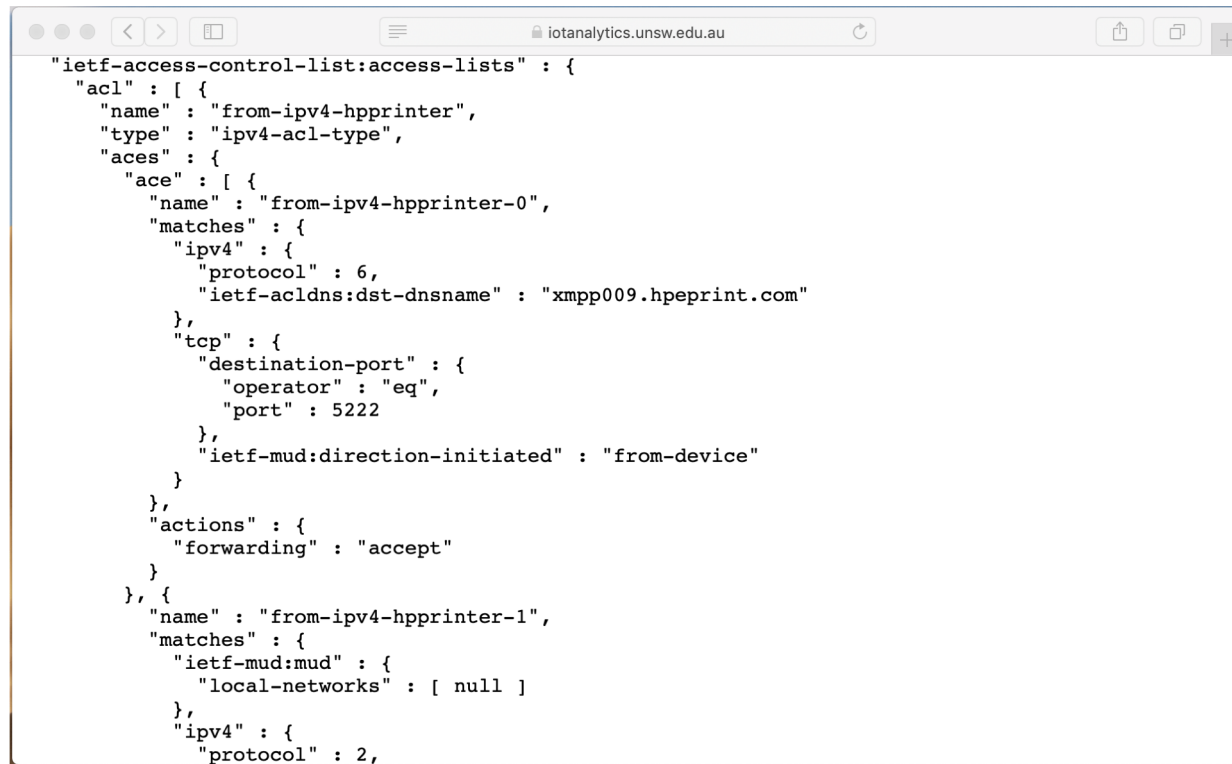
**Some Samples**

A device that just needs to talk to a single cloud service	<a href="#">Cloud Service</a>
A device that just needs to talk to its local controllers	<a href="#">My Controller</a>
A device that just needs to talk to devices from the same manufacturer	<a href="#">Same Manufacturer</a>

If you use the samples, you will need to modify some of the fields, and of course sign them.

**Make Your Own!**

So for instance...

A screenshot of a web browser window. The address bar shows 'iotanalytics.unsw.edu.au'. The main content area displays a JSON snippet. The JSON is a list of ACLs under the key 'ietf-access-control-list:access-lists'. The first ACL is named 'from-ipv4-hpprinter' and has two entries in its 'aces' array. The first entry is named 'from-ipv4-hpprinter-0' and matches traffic from protocol 6 (TCP) to destination port 5222 on the host 'xmpp009.hpeprint.com'. The second entry is named 'from-ipv4-hpprinter-1' and matches traffic from local networks. The browser window has standard macOS window controls (red, yellow, green buttons) and a plus sign in the top right corner.

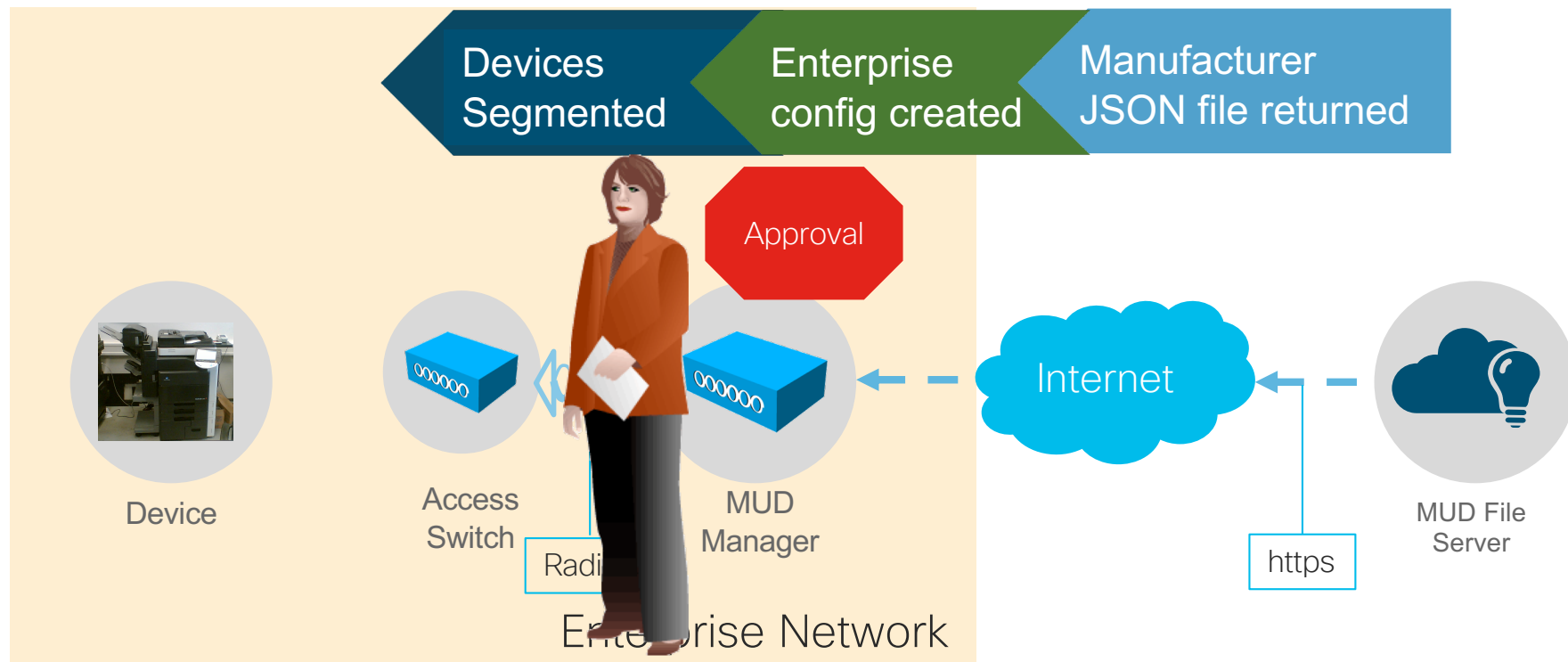
```
"ietf-access-control-list:access-lists" : {  
  "acl" : [ {  
    "name" : "from-ipv4-hpprinter",  
    "type" : "ipv4-acl-type",  
    "aces" : {  
      "ace" : [ {  
        "name" : "from-ipv4-hpprinter-0",  
        "matches" : {  
          "ipv4" : {  
            "protocol" : 6,  
            "ietf-acldns:dst-dnsname" : "xmpp009.hpeprint.com"  
          },  
          "tcp" : {  
            "destination-port" : {  
              "operator" : "eq",  
              "port" : 5222  
            },  
            "ietf-mud:direction-initiated" : "from-device"  
          }  
        },  
        "actions" : {  
          "forwarding" : "accept"  
        }  
      }, {  
        "name" : "from-ipv4-hpprinter-1",  
        "matches" : {  
          "ietf-mud:mud" : {  
            "local-networks" : [ null ]  
          },  
          "ipv4" : {  
            "protocol" : 2,  

```

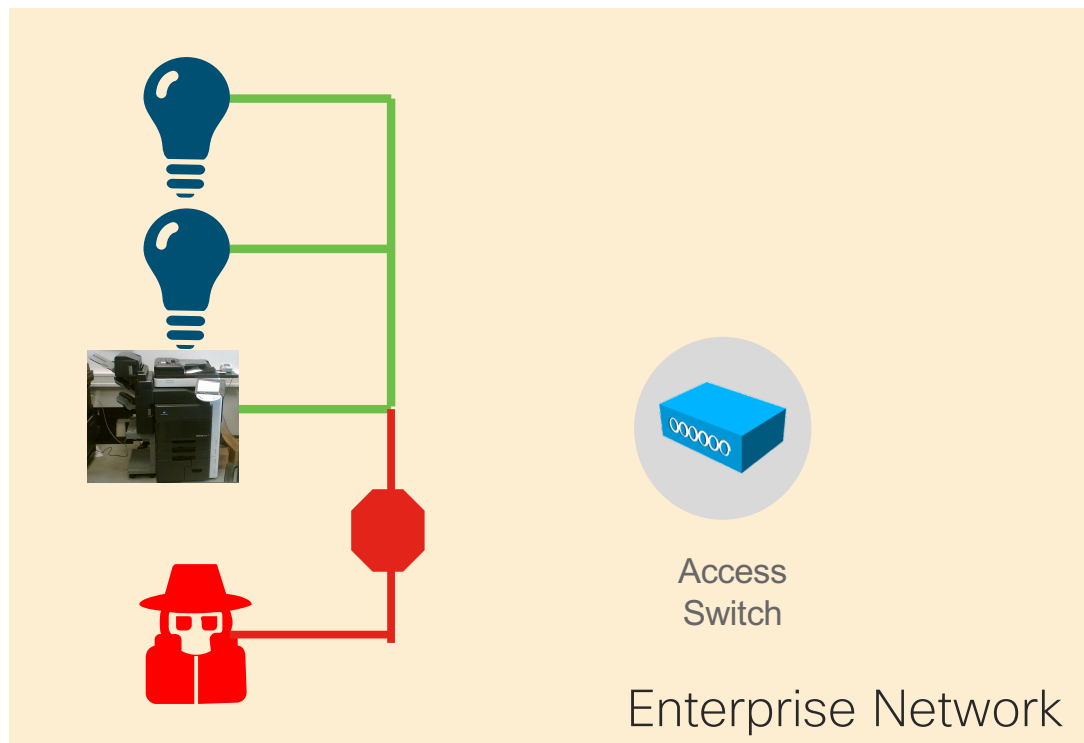
(Just a snippet)



# Expressing Manufacturer Usage Descriptions



## Results: Micro-segmentation of that printer



- Access limited to devices based on manufacturer recommendations
- Policy choices easily identified by MUD file
- Hacked devices can't probe for holes
- An additional layer of security
  - BUT- manufacturers should still **always** secure their devices

# Next Steps

- More MUD tooling
- MUD for 5G
- More implementations!

Thank You!

© 2019 Cisco and/or its affiliates. All rights reserved.



# Credit to... (Creative Commons Licensing)

- The Printer  
<https://en.wikipedia.org/w/index.php?curid=16404543>



